SunScreen EFS 3.0 Revision B Stealth Mode Operation

Security Target

July 24, 2000
Arca LTEF 002/2000 Sun SMST Final

Submitted to
Sun Microsystems
901 San Antonio Road
Palo Alto, CA 94303-4900

Submitted by
Arca Systems, Inc.
An Exodus Communications Company
10220 Old Columbia Road, Suite G-H
Columbia, MD 21046

`http://www.arca.com`

TABLE OF CONTENTS

1 Introduction

This introduction provides the necessary information to uniquely identify the Target of Evaluation (TOE) and its associated Security Target.

This Security Target describes the Sun Microsystems SunScreen EFS 3.0 revision B Stealth mode TOE submitted for evaluation.

1.1 Identification

TOE Identification:	Sun Microsystems, SunScreen EFS 3.0 Revision B, Stealth Mode Operation
PP Identification:	None.
ST Identification:	Sun Microsystems, SunScreen EFS 3.0 Revision B Security Target, Arca LTEF 002/2000 Stealth Mode
Keywords:	Firewall, Screen, Access Control, and Network Security.
Published:	24 July 2000
Authors:	Arca Systems LTEF

1.2 Overview

SunScreen EFS is a software package that is installed on a Solaris-based machine to allow customers to connect their departmental networks to public networks in a secure manner. SunScreen EFS can function as a firewall and a router for hosts on the network it is protecting.

SunScreen EFS allows division of a network into discrete areas, each served by an interface that provides customized fine-grain access control. Using filtering rules, SunScreen EFS controls the access from one area of a network to another, as well as access to the Internet or other external networks. A typical architecture is shown in Figure 1.

SunScreen EFS consists of a rules-based, dynamic packet-filtering engine for network access control, and an encryption and authentication engine that enables the creation of virtual private network (VPN) gateways by integrating public-key encryption technology. SunScreen also offers high availability (HA) for standards-based encryption. SunScreen EFS is administered through a graphical user interface (GUI) via a secure Web browser connection.

SunScreen EFS has two modes of operation: Routing, or Stealth. In **Routing Mode**, SunScreen EFS operates as both a router and an application-level firewall and is visible on both the internal and external networks. In **Stealth Mode**, the SunScreen EFS does not have the capabilities of a router, but instead acts as a bridge transparently passing packets through the *Screen* which in this instance is a straight traffic-filter firewall. It is not visible either on the internal or external networks.

In SunScreen EFS there are two main functional components, the Screen and the Administration Station. The Screen is composed of the firewall responsible for filtering packets according to the security policy being enforced and SKIP. Simple Key Management for Internet Protocols (SKIP) is used within the TOE to provide the encryption between the remote Administration Station and the Screen. The Administration Station is used to define the rules specified by the security policy, and to administer the Screen. The number of Screens and Administration Stations depends upon the user site network topology and security policies.

Local Administration means that the Administration Station is resident on the same machine as the Screen itself. Since no network traffic is generated between the Administration Station and the Screen, local administration does not require, nor utilize, encryption.

Remote Administration means that administration of the Screen is conducted on an Administration Station which is a separate machine from the Screen, as shown in Figure 1-2.

Remote Administration uses encrypted communication between the Screen and the Administration Station to protect access and to limit the management of a Screen to an authorized Administration Station. The data which the administrator sees is protected, so the information about the security policy in place on the Screen cannot be obtained by others. The Simple Key Management for Internet Protocols (SKIP) is used within the TOE to provide the encryption between the remote Administration Station and the Screen.

SunScreen SKIP provides hosts that use the Solaris operating system with the ability to encrypt any protocol within the TCP/IP protocol suite. The TOE requires installation of the SunScreen SKIP to allow the capability of remote administration.

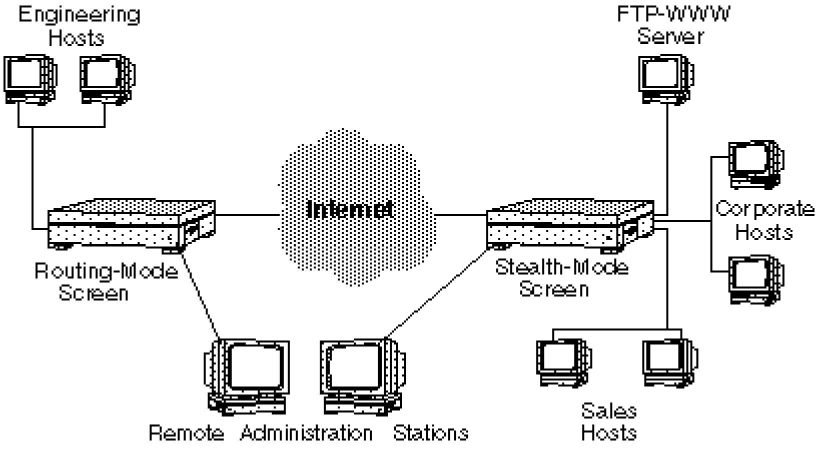


FIGURE 1 The diagram above illustrates a simple network, with SunScreen Secure Net protecting various areas of a company's network infrastructure.

1.3 CC Conformance Claim

The TOE is Common Criteria Version 2.1 (ISO/IEC 15408:1999) Part 2 and Part 3 conformant at EAL2.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	Functional and Assurance Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims

Table 1-1: ST Organization and Description

1.5 Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of the Security Target.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user Any person who interacts with the TOE.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication data Information used to verify the claimed identity of a user.

From the above definitions given by the CC, the following terms can be derived:

Authorized external IT entity Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized Administrator A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

2 TOE Description

2.1 Overview

The generic SunScreen EFS product allows the use of routing mode interfaces that enable the use of proxies. For this TOE, only the stealth mode firewall configuration is permissible. The TOE acts as a traffic-filtering firewall without proxies.

The Stealth mode SunScreen EFS installation provides the option of hardening the system. Hardening automatically removes Solaris files and packages that might make the TOE vulnerable. Once hardened, the TOE becomes a dedicated firewall and the system cannot be used for another purpose without reinstalling the operating system. For this TOE, the system will be hardened.

SunScreen EFS consists of two main components: a Screen and its Administration Station. The Screen component is responsible for filtering packets according to the established policy and initiating SKIP operations. The policy is administered from a remote Administration Station. During installation, the administrator is instructed to configure only the network interface that will be used for remote administration. Configuring additional network interfaces is not supported. The two components can be installed on a single machine for local administration, but this configuration is not recommended or supported in stealth mode and is not part of the TOE.

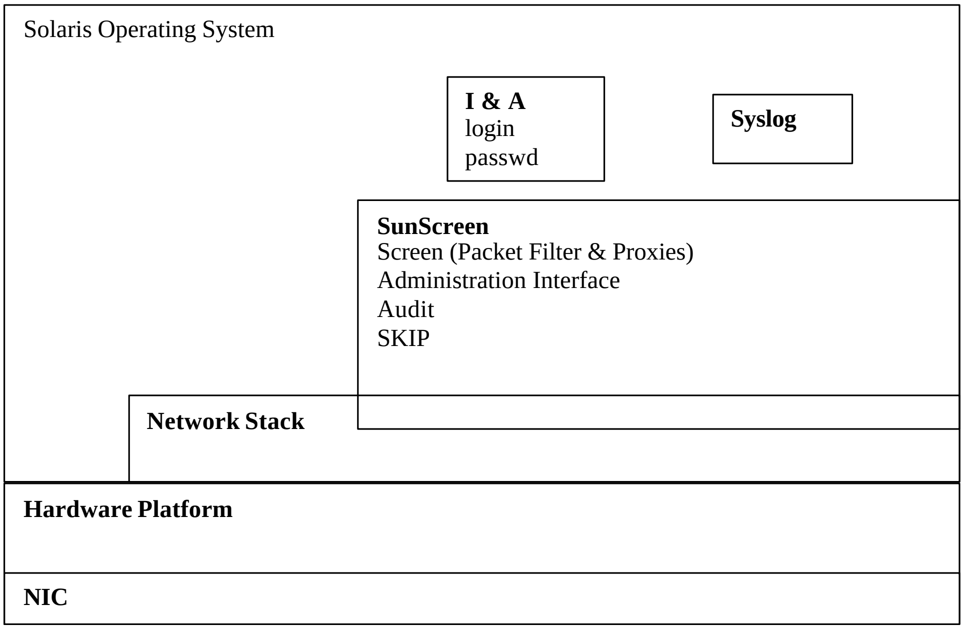
Remote administration traffic is protected via an encrypted path using the SunScreen SKIP protocol.

The TOE consists of the following software components:

Solaris 2.6 or Solaris 7 operating system	Identification & Authentication Syslog Network Stack
SunScreen	Screen Administrative Interfaces High Availability Audit SKIP 1.5
SecurID client	Compatible with ACE/Server version 3.0.1.

The hardware components of the TOE are identified in the Table in Section 2.2.

The following block diagram provides a graphical representation of the TOE.



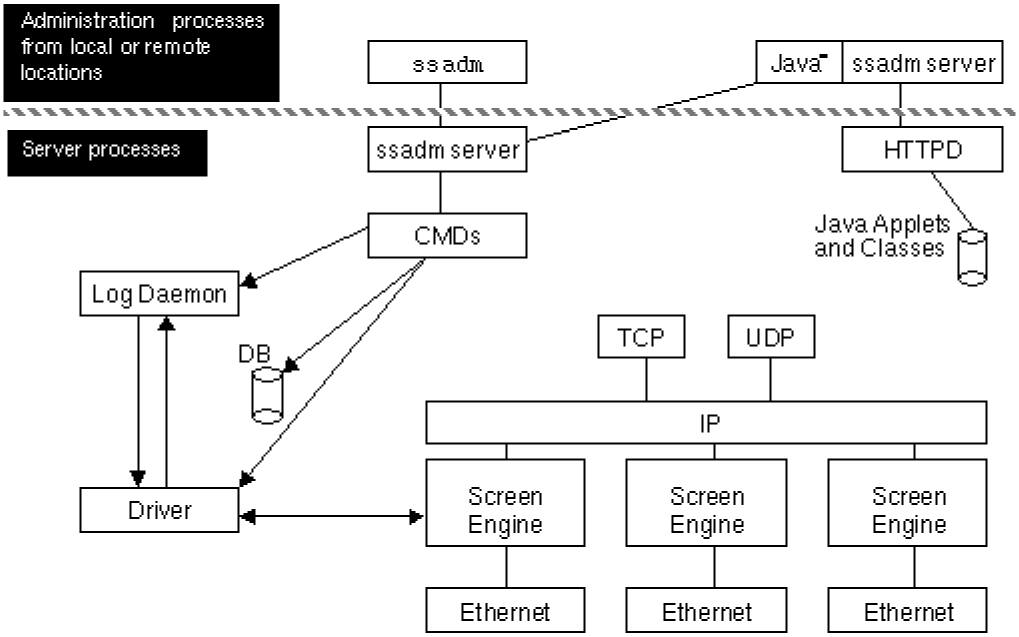
2.2 Hardware/OS Components

Operating System	Solaris 7 or 2.6 Operating Environment for SPARC and Intel Platforms
Web Browser	HotJava 1.1.5
Firewall Software	SunScreen EFS 3.0 Revision B, includes all software packages required on the Screen to implement the TOE.
Third Party Software	SecurID (SunScreen EFS is compatible with ACE/Server version 3.0.1 and higher)
Hardware	All SPARC and UltraSPARC platforms developed to the SPARC version 9 specification, and 486 and Pentium Intel platforms supported by the Solaris 7 and 2.6 Operating Environments.
Disk Space	Minimum of 1 Gbyte (>300Mbytes free)
Memory	Administration: Minimum of 32Mbytes, 64 Mbytes strongly recommended.
Network Interfaces	For SPARC systems: 10-Mbps or 100-Mpbs Ethernet Interfaces (le, qe, hme, be, qfe)*. For Intel systems: 10 Mbps or 100 Mbps Ethernet Interfaces (dnet, elxl)*. HA requires that the two boxes be connected in a non-switched hub. *Any NICs on the corresponding Sun Hardware Compatibility Lists: Hardware Compatibility List for Solaris 2.6, April 2000. Solaris 7 Hardware Compatibility List, June 2000.

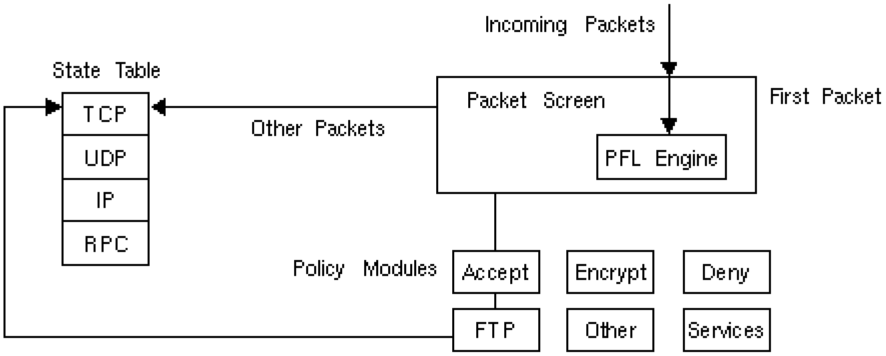
Media	CD-ROM drive and diskette drive
High Availability (HA)	All Screens in a HA network must have identical hardware network interface cards.

2.3 Architecture Description

SunScreen EFS comprises a set of interrelated processes, operating together in a modular architecture as shown below.



The TOE is administered remotely through either a command line interface using the ssadmin command or through a GUI interface with a Java-technology enabled browser. The commands from the ssadm server control the log module and a driver module that controls the packet screen. The driver downloads packet filter (PFL) configurations into each engine, and makes log entries of the processes as they execute. The SunScreen EFS packet screen is layered between the TCP/IP layers and the Ethernet layer of the kernel. Multiple engines can reside in the kernel.



The packet screen contains a PFL engine. The PFL engine includes a PFL compiler that generates PFL code. Processes called “policies” are general action categories for accepting and denying actions, as well as SKIP encryption. The PFL engine distills policies and actions into code. The State Table lists all active TCP connections, including the owners of the connections. The tables are reset only upon reboot.

2.3.1 Packet Flow

A packet travels through the Ethernet interface and into the packet screen. The packet screen is located between the Ethernet interface and the operating system. The first packet is directed to the PFL engine that passes it through the rule base. If the packet is passed, it is sent to the applicable policy module. If it passes this module, it is directed to the appropriate protocol engine, such as FTP engine for an FTP connection. The FTP (or other protocol) engine makes an entry in the state table indicating a new TCP connection has been established, is ready for communication, and the FTP state engine owns it. Subsequent packets from the established connection are sent directly to the state table, and not the PFL engine, to verify that they are part of a TCP connection has already been approved.

2.4 TOE Functional Component Description

The TOE software components consist of the Solaris operating system, SunScreen, and SecurID client. The SunScreen component is comprised of five subcomponents: Screen, Administrative Interfaces, High Availability, Audit, and SKIP.

2.4.1 Solaris

SunScreen EFS relies on the Solaris operating system as the basis for providing its security. The Solaris kernel provides the following basic security and operating system functions:

process isolation	proper separation of data during each network connection

object reuse	network packets do not contain residual data
system time	provides the system time
identification and authentication	provides user authentication for users locally accessing the system via the console and for users requesting to modify their authentication information
audit	provides the ability to log security-relevant events via syslog
network stack	provides the foundation for all network activities and network security

2.4.2 SunScreen

2.4.2.1 Screen

The screen component is the firewall layered between the TCP/IP and Ethernet layers of the kernel. The screen is responsible for monitoring, filtering, encrypting, and decrypting basic IP network traffic.

2.4.2.1.1 Dynamic Packet Filtering

Dynamic packet filtering sits between the client and server and examines each data packet as it arrives. Based on information in the packet, state retained from previous events, and a set of security policy rules, the data packet is either passed or blocked and dropped.

SunScreen EFS uses a set of ordered rules to filter packets. When SunScreen is configured, security policies are translated for the site into a series of policy rules that specify which services are to be allowed, what to do with packets for services that are disallowed, and what to do when packets are dropped. Placing these policy rules in sequence specifies which rules override others.

2.4.2.1.2 Network Address Translation (NAT)

Network Address Translation (NAT) enables a Screen to map an internal network address to a different network address. As it passes packets between an internal host and a public network, the addresses in the packet are replaced with new addresses transparently, checksums and sequence numbers are corrected, and the state of the address map is monitored. Application of ordered NAT translations is based on the presumed source or destination address of the packet.

Additionally, services such as FTP also carry IP address information. These packets must also be changed, ensuring that the checksums and sequence numbers are correct. All of this is done inside the Screen’s kernel to ensure high-speed processing and transparency to the end user and applications.

2.4.2.1.2.1 Static NAT

Static NAT maps a specific unregistered address to a specific registered address. Static translations can also map a range of unregistered addresses to a range of registered addresses, requiring the number of addresses in each range to match.

Registered addresses are necessary for advertised kinds of resources such as publicly accessible servers on the network. Static NAT is used to provide public access to HTTP or FTP servers that use private addresses.

2.4.2.1.2.2 Dynamic NAT

Dynamic NAT maps a large set of unregistered IP addresses to a smaller set of registered addresses. It provides external connections for a very large number of hosts to the public Internet using a limited number of registered addresses. Dynamic NAT creates a one-to-many mapping where several internal addresses use the same public address. Dynamic NAT avoids IP address conflicts by maintaining a state table that records five values (source address, source port, destination address, destination port, and protocol) for each TCP or UDP connection.

Dynamic NAT is unidirectional, which means that communication can be initiated only internally from within the unregistered private network. So only a user from inside the firewall can originate a connection. Packets received from the outside that are not in the address lookup table of an established connection cannot be identified and are discarded.

2.4.2.2 High Availability (HA)

HA contributes to protecting against denial of service attacks and enables the deployment of multiple screens in situations where the connection between a protected inside network and an insecure outside network is required. One member of the HA cluster, the active HA screen, performs packet filtering, network address translation, logging, and encryption/decryption of packets traveling between the inside and outside networks. The other members of the HA cluster (up to 31 passive screens), receive the same packets, perform the same calculations and mirror the state of the active HA screen, but they do not forward traffic. If the active HA screen fails, one of the passive screens takes over as the active and begins routing and filtering network traffic. This results in few lost connections in the event of screen failure.

2.4.2.3 Audit

SunScreen EFS provides flexible logging of packets based upon configured parameters. Packets may be logged if they do or do not match a particular rule. For any given program component, the level of logging can be specified. The value of the log size and information to be recorded in the administrative log files is established during the setup of SunScreen EFS.

2.4.2.4 SKIP

SunScreen SKIP is an IP-layer encryption package integrated into SunScreen EFS. SunScreen SKIP is based on the Simple Key-management for Internet Protocols standard for key management for IP encryption. SunScreen SKIP operates at the network (IP) layer and is transparent to virtually all applications. Secure communication is possible with all IP (both TCP and UDP) applications without modification or knowledge of SKIP[1].

Virtual Private Networks (VPNs) and remote administrative traffic use the same SKIP mechanisms to provide secure communication.

2.4.2.4.1 Virtual Private Networks

SunScreen EFS enables you to create Secure Virtual Private Networks over public, insecure networks, such as the Internet. Encrypted tunnels protect the data transmitted between SKIP-enabled hosts or users, preventing unauthorized access to private data. The administrator selects what type of private-key and bulk-data encryption is to be used (such as RC2, RC4 or DES). For maximum security, SunScreen EFS uses SunScreen SKIP and Diffie-Hellman key pairs to encrypt the traffic key used for the bulk-data encryption and change the traffic key at frequent intervals

SKIP provides transparent encryption and authentication, which automatically encrypts and decrypts messages exchanged with other hosts running SKIP to ensure message privacy.

The TOE includes the SunScreen EFS firewall end point of the tunnel and does not include the other end point. The TOE protects its own endpoint and is capable of being an initial or terminating end point. This evaluation addresses the audit, authentication, and access control features of VPN traffic. It does not address the confidentiality of VPN traffic over a public network.

VPNs are implemented using the encryption action of the packet filtering rules. The simplest rule allows encrypted use of the specified service for all addresses in the VPN. The rules allow the administrator to select the set of algorithms to be used by the VPN.

2.4.2.5 Administrative Interface

SunScreen EFS allows secure, web based administration. The administration tasks are performed from a remote workstation. All administrative configuration is performed over a SKIP encrypted link on the only configured network interface on the firewall.

The SunScreen EFS administration GUI uses Java applets to administer and monitor Screens.

[1] SKIP was developed by Sun Microsystems, Inc. and the technology has been placed into the public domain to ensure interoperability between multiple implementations, including the SunScreen product line.

The Java code on the browser runs in a Java sandbox and the JVM on a Screen only executes Java code from the local file system, not the network. Communication between a screen and an administration station are protected by SKIP encryption and require an Admin SKIP certificate.

SunScreen EFS provides centralized management of multiple Screens using a set of common objects through a specific, primary Screen. An administrator can also monitor logs on individual Screens or monitor logs of a centralized management group.

Many different Administration stations can manage the primary Screen. There is no defined limit to the number of different Administration stations that can manage the primary Screen. SunScreen EFS provides a locking mechanism that is used to prevent multiple administration stations from simultaneously editing policies on the same screen. The policy list page can be locked for modification when opened by an administrator. Other administrators are allowed to view the policy lists when another administrator has locked them. The lock is released when the administrator saves their changes or logs out of the administration interface.

A Command Line Interface is available to administer the screen from the screen's console. The ssadm command contains a number of parameters that encompass the tasks performed using the GUI.

2.4.3 SecurID ACE/Client

SecurID authentication is an optional means of user authentication. Used with the RSA ACE/Server®[2], the SecurID token generates a new, unpredictable access code every 60 seconds.

ACE/Server provides centralized, strong authentication services, ensuring that only authorized users gain access to resources. ACE/Server lets you create a secure perimeter around your network, ensuring that only authorized users are permitted to enter beyond the network perimeter.

SecurID uses a two-factor authentication scheme. One factor is a pseudo-random number generator. The second factor is a personal identification number (PIN). SecurID utilizes encryption and authentication mechanisms that are proprietary to RSA Security, Inc. With ACE/Server and SecurID, only those with the correct combination of the user's PIN and token code will be allowed access to the network. SecurID authentication ensures that a particular token is associated with a specific SunScreen user. Configuration of SecurID authentication is performed using the SunScreen administrative interfaces.

The SunScreen authentication mechanism provides a client interface to the RSA SecurID token card. The SecurID ACE/Server manages the username/SecurID tokens. The SecurID ACE/Client resides within the proxy authentication and administrative interface modules. Use of SecurID requires at least one external SecurID ACE/Server. SunScreen EFS does not provide a SecurID

[2] Both RSA SecurID and RSA ACE/Server were formerly produced by Security Dynamics.

ACE/Server.

With the addition of SecurID to the TOE, the methods of authentication are:

- username and password
- username, PIN, and tokencode
- username and a combination of password and PIN/tokencode

2.5 Product Features

The SunScreen EFS product consists of additional product features that are not included as part of the TOE. These product features include:

- Web Browsers

2.5.1 Web Browsers

The only web browser evaluated as part of the TOE is HotJava 1.1.5. Other browsers mentioned below are compatible with the product but are not included as part of the TOE.

SunScreen EFS requires a Java technology-enabled Web browser compliant with JDK 1.1.3 or later that can securely connect using SKIP.

Netscape Communicator 4.5 and Internet Explorer 4.01 can be used to perform all administrative functions except those requiring local file access.

SKIP software is used with Java technology enabled browsers for remotely administering SunScreen screens. SKIP software is available for the Solaris Operating Environment.

3 TOE Security Environment

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

A.PHYSEC The TOE is physically secure.

A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

A.SECURID The SecurID ACE/Server is physically secure. In addition, it is administered and maintained in accordance with standard security practices and vendor provided documentation.

3.2 Threats

The TOE or the environment addresses the following threats.

3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.ASPOOF An unauthorized person may carry out spoofing in information flows mediated by the TOE between clients and servers located on internal and external networks governed by the TOE, by using a spoofed source address.

T.MEDIAT An unauthorized person may send impermissible information through the TOE that results in the exploitation of resources on the internal network.

T.OLDINF Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

3.2.2 Threat to be Addressed by Operating Environment

Procedural measures and/or administrative methods counter the threat possibilities described below.

T.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

4 Security Objectives

4.1 Information Technology (IT) Security Objectives

The following are the IT security objectives for the TOE:

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.MEDIAT The TOE must mediate the flow of all information between users on an internal network connected to the TOE and users on an external network connected to the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

4.2 Security Objectives For The Environment

All the assumptions stated in this section are considered security objectives for the environment. The following list consists primarily of the non-IT security objectives for the environment, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

The last three objectives in this list consist of security objectives for the environment which do result in IT security requirements on the environment. These objectives relate to the SecurID server, that are not included within the TOE, but which the TOE relies upon to provide accurate information to make security related decisions.

O.PHYSEC The TOE is physically secure.

O.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

O.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

O.PUBLIC The TOE does not host public data.

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

O.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

O.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

O.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

O.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

O.SECURID The information provided by the SecurID ACE/Server is reliable.

O.EXTAUTH External Third Party authentication servers are securely installed, configured, administered and are physically protected.

4.3 Rationale For IT Security Objectives

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats.

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF that have to do with getting impermissible information to flow through the TOE. This security objective requires that the TOE mediates all information that passes through the networks and that no residual information is transmitted.

O.SECSTA This security objective ensures that no information is compromised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

O.ENCRYP This security objective is necessary to counter the threats: T.ASPOOF, T.NOAUTH and T.PROCOM by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.

	T.NOAUTH	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL
O.IDAUTH	X							
O.MEDIAT		X	X	X				
O.SECSTA	X						X	
O.ENCRYP	X	X			X			
O.SELPRO							X	X
O.AUDREC						X		
O.ACCOUN						X		
O.SECFUN	X							X
O.LIMEXT	X							

Table 8.1 – Summary of Mappings Between Threats and IT Security Objectives

4.4 Rationale For Security Objectives For The Environment

This section provides the rationale that all security objectives for the environment are traced back to aspects of the addressed threats or assumptions.

The following security objectives for the environment are, in part, a re-statement of all the security assumptions and therefore cover all aspects of the assumptions.

O.PHYSEC The TOE is physically secure.

O.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

O.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

O.PUBLIC The TOE does not host public data.

O.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

O.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

O.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

O.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

O.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

O.SECURID The SecurID ACE/Server is physically secure and administered according to RSA security guidance so the information provided is reliable.

The following security objectives for the environment do not trace to assumptions.

O.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner. It also covers T.AUDACC by requiring that the TOE will be administered and operated in a secure manner, which includes reviewing audit records.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training.

O.EXTAUTH This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators install, configure, administer, and operate external third party authentication servers in a secure manner.

	T.TUSAGE	T.AUDACC
O.GUIDAN	X	X
O.ADMTRA	X	
O.EXTAUTH	X	

Table 8.2 - Summary of Mappings Between Threats and Non-IT Security Objectives

4.5 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.NOAUTH Countering this threat involves authenticating users, enforcing access rules to non-security functions, security functions and authorized network communications. O.IDAUTH counters this threat by ensuring that users uniquely identify themselves prior to accessing the TOE. O.SECSTA counters this threat by ensuring that the TOE does not compromise resources during start-up or recovery. O. ENCRYP counters this threat by ensuring that encryption is used to remotely administer the TOE. O.SECFUN counters this threat by ensuring that only authorized administrators have access to TOE security functions. O.LIMEXT covers this threat by requiring that the TOE provide the ability to control and limit access to TOE security functions.

T.ASPOOF Countering this threat involves ensuring that the TOE mediates all network traffic and when required authenticates the originator of the network traffic. O.MEDIAT counters this threat by ensuring that the TOE mediates all network traffic. O.ENCRYP counters this treat by requiring the use of encryption to administer the machine remotely.

T.MEDIAT Countering this threat involves ensuring that the TOE mediates all network traffic. O.MEDIAT counters this threat by ensuring that the TOE mediates all network traffic.

T.OLDINF Countering this threat involves ensuring that residual is not accessible for future information flows. O.MEDIAT counters this threat by ensuring residual information from a previous information flow is not transmitted.

T.PROCOM Countering this threat involves ensuring that security related information sent over the network is encrypted. O.ENCRYP covers this threat by requiring the use of encryption for remote administration functions.

T.AUDACC Countering this threat involves ensuring accountability for action by auditing and reviewing the actions. O.AUDREC covers this threat by requiring a readable audit trail and a method for searching and sorting the audit records. O.ACCOUN covers this threat by requiring accountability for information flows through the TOE and the use of security functions. O.GUIDAN covers this threat by requiring that the TOE will be administered and operated in a secure manner, which includes reviewing audit records.

T.SELPRO Countering this threat involves controlling access to TOE configuration data at all times. O.SECSTA covers this threat by ensuring that during startup and recovery, the TOE does not compromised any information. O.SELPRO covers this threat by requiring that the TOE protect itself from attempts to bypass, deactivate, or tamper with its security functions.

T.AUDFUL Countering this threat involves controlling access to TOE audit trail and protecting the TOE audit functions. O.SELPRO covers this threat by requiring that the TOE protect itself from attempts to bypass, deactivate, or tamper with its security functions. O.SECFUN covers this threat by ensuring that only authorized administrators have access to TOE security functions.

T.TUSAGE Countering this threat involves secure configuration, usage, and administration of the TOE. O.GUIDE covers this threat by requiring that personnel responsible for the TOE ensure secure delivery, installation, administration, and operation. O.ADMTRA covers this threat by ensuring that administrators attend proper training. O.EXTAUTH covers this threat by requiring that personnel responsible for external third party authentication servers ensure secure installation, configuration, administration, and operation.

4.6 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

All the security assumptions have been restated, in part, as security objectives for the environment. Therefore, the corresponding security objectives for the environment cover all aspects of the assumptions.

5 IT Security Requirements

5.1 TOE Security Requirements

This section provides functional and assurance requirements satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1.1 TOE Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, summarized in the following table.

Functional Components	
FMT_SMR.1	Security roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.1	Management of security attributes (1)
FMT_MSA.1	Management of security attributes (2)
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data (1)
FMT_MTD.1	Management of TSF data (2)
FDP_RIP.1	Subset residual information protection
FCS_COP.1	Cryptographic operation (1)
FCS_COP.1	Cryptographic operation (2)
FCS_COP.1	Cryptographic operation (3)
FCS_COP.1	Cryptographic operation (4)
FCS_COP.1	Cryptographic operation (5)
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of Security Functions Behavior
FRU_FLT.1	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state

Table 5.1 - Functional Requirements

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism. In the case of this ST, this minimum level shall be SOF-basic. For a rationale for this selected level, see section 5.2.1, “Rationale For Security Functional Requirements”.

Specific strength of function (SOF) metrics defined for the FIA_UAU.1 security functional requirements are:

Strength of function shall be demonstrated for the mechanism used by the TOE to meet

FIA_UAU.1 in that the probability that authentication data can be guessed is no greater than one in one million (1/E6).

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***Status, Local, Executive and Master administrators***.

FMT_SMR.1.2 The TSF shall be able to associate users with roles. .

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) ***identity;***

b) ***group identity/identities;***

c) ***association of a human user with the authorized administrator role;***

d) authentication information (such as passwords, pins or tokens)**.**

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing **any other TSF-mediated actions** on behalf of that user.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***information flow control decisions and subsequent passing or dropping of packets in support of the identification and authentication process*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***UNAUTHENTICATED SFP***[3] on:

a) ***subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;***

b) ***information: traffic sent through the TOE from one subject to another;***

c) ***operation: pass information.***

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the ***UNAUTHENTICATED SFP*** based on at least the following types of subject and information security attributes:

a) ***subject security attributes:***

- ***presumed address;***

b) ***information security attributes:***

- ***presumed address of source subject;***
- ***presumed address of destination subject;***
- ***transport layer protocol;***
- ***TOE interface on which traffic arrives and departs;***
- ***service;***
- ***certificate for encryption;***
- ***time of day;***

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) ***Subjects on an internal network can cause information to flow through the TOE to another connected network if:***

- ***all the information security attribute values are unambiguously permitted by the information flow security***

[3] For the Stealth mode version of SunScreen EFS, the UNAUTHENTICATED SFP is the packet filter.

policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

- ***the presumed address of the source subject, in the information, translates to an internal network address;***
- ***and the presumed address of the destination subject, in the information, translates to an address on the other connected network.***

b) ***Subjects on the external network can cause information to flow through the TOE to another connected network if:***

- ***all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;***
- ***the presumed address of the source subject, in the information, translates to an external network address;***
- ***and the presumed address of the destination subject, in the information, translates to an address on the other connected network.***

FDP_IFF.1.3 The TSF shall enforce the ***no additional information flow control SFP rules***.

FDP_IFF.1.4 The TSF shall provide the following ***no additional SFP capabilities***.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: ***none***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) ***The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;***

b) ***The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the***

presumed address of the source subject is an external IT entity on the external network;

c) ***The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;***

d) ***The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network***

e) ***The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject;***

f) ***The TOE shall reject malformed service requests.***

FMT_MSA.1 Management of security attributes (1)

FMT_MSA.1.1(1) The TSF shall enforce the ***UNAUTHENTICATED_SFP*** to restrict the ability to ***add attributes to a rule, delete attributes from a rule, modify attributes in a rule, change*** the security attributes ***listed in section FDP_IFF1.1(1)*** to ***the Executive or Master administrators***.

FMT_MSA.1 Management of security attributes (2)

FMT_MSA.1.1(2) The TSF shall enforce the ***UNAUTHENTICATED_SFP*** to restrict the ability to ***create and delete*** the security attributes ***listed in information flow rules described in FDP_IFF.1(1)*** to ***the Executive or Master administrator***.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the ***UNAUTHENTICATED_SFP*** to provide ***restrictive*** default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***Executive or Master administrator*** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data (1)

FMT_MTD.1.1 (1) The TSF shall restrict the ability to ***query, modify, delete, and assign*** the ***user's identity and group identity*** to ***the Master administrator***.

FMT_MTD.1 Management of TSF data (2)

FMT_MTD.1.1 (2) The TSF shall restrict the ability to ***set*** the ***time and date used to form the timestamps in FPT_STM.1.1*** to ***the Master administrators***.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon ***the allocation of the resource from*** the following objects: ***packets, buffers, and configuration rules***.

FCS_COP.1 Cryptographic operation (1)

FCS_COP.1.1 (1) The TSF shall perform ***encryption and decryption of remote authorized administrator sessions*** in accordance with a specified cryptographic algorithm ***DES-CBC*** and cryptographic key sizes ***of 56-bit*** that meet the following: ***FIPS PUB 46-2 [3] and FIPS PUB 81 [4]***.

FCS_COP.1 Cryptographic operation (2)

FCS_COP.1.1 (2) The TSF shall perform ***encryption and decryption of remote authorized administrator sessions*** in accordance with a specified cryptographic algorithm ***DES-EDE-K3 (Triple DES)*** and cryptographic key sizes ***of 56-bit*** that meet the following: ***FIPS PUB 46-2 [3] and FIPS PUB 81 [4]***.

FCS_COP.1 Cryptographic operation (3)

FCS_COP.1.1 (3) The TSF shall perform ***encryption and decryption of remote authorized administrator sessions*** in accordance with a specified cryptographic algorithm ***RC2-40*** and cryptographic key sizes ***variable*** that meet the following: ***RSA standard***.

FCS_COP.1 Cryptographic operation (4)

FCS_COP.1.1 (4) The TSF shall perform ***encryption and decryption of remote authorized administrator sessions*** in accordance with a specified cryptographic algorithm ***RC4-128*** and cryptographic key sizes ***of 128-bit*** that meet the following: ***RSA standard***.

FCS_COP.1 Cryptographic operation (5)

FCS_COP.1.1 (5) The TSF shall perform ***encryption and decryption of remote authorized administrator sessions*** in accordance with a specified cryptographic algorithm ***RC4-40*** and cryptographic key sizes ***of 40-bit*** that meet the following: ***RSA standard***.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***namely, Diffie-Hellman*** and specified cryptographic key sizes ***512, 1024, and 2048-bit key sizes*** that meet the following: ***Public Key Cryptography Standard #3 (PKCS #3), Diffie-Hellman Key Agreement Standard***.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***overwriting*** that meets the following: ***SKIP***.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***not specified*** level of audit**;** and

c) The events listed in Table 5.2.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subjects identities, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[information specified in column four of Table 5.2]***.

Functional Component	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FCS_COP.1	Success and failure, and the type of cryptographic operation	The identity of the external IT entity attempting to perform the cryptographic operation
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

Table 5.2 - Auditable Events

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***the Status, Local, Executive, and Master administrators*** with the capability to read ***all audit trail data*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform ***searches and sorting*** of audit data based on:

a) time

b) date

c) types of events (e.g., packet-type, session-type, authentication, severity-type);

d) logging reason code;

e) arrival interface;

f) hostname;

g) service name;

h) network;

i) gateway used;

j) protocol type (i.e., UDP, TCP, ICMP, or RPC).

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** modifications to the audit records.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall ***overwrite the oldest stored audit records*** and ***no other actions to be taken in case of audit storage failure*** if the audit trail is full.

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by all authorized administrators and shall limit the number of audit records lost if the audit trail is full.

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behavior of, disable, enable, modify the behavior of*** the functions ***listed in the following table to authorized roles identified in the following table***.

ABILITIES	FUNCTION	AUTHORIZED ROLE
	Start the TOE.	Master Administrators
	Shutdown the TOE.	Master Administrators
Enable/Disable	information flow security policy rules that permit or deny information flows.	Executive or Master Administrators
Determine the behavior/ Modify the behavior/ Disable/ Enable	user attribute values defined in FIA_ATD.1.	Master Administrators
Enable/Disable	external IT entities communicating with the TOE.	Executive or Master Administrators
Enable/Disable	Single use authentication	Executive or Master Administrators
Enable/Disable	Remote administration from either an internal or external network	Executive or Master Administrators
Enable/Disable	Addresses for remote administration	Executive or Master Administrators
Enable/Disable	Assignment of individuals from being authorized remote administrators	Master Administrators
Enable/Disable	Access levels for remote administrators	Master Administrators
Modifying the behavior	Data and Time function	Master Administrators
	View the Audit Trail.	Any Administrator
Enable/Disable	Audit Trail to include archiving, creating, deleting and emptying.	Master Administrators
Enable/Disable	Backup of user attribute values, information flow security policy rules, and audit trail data.	Master Administrators
	Recover to the state following the last backup	Master Administrators
Enable/Disable	Communication of authorized external IT entities with the TOE	Executive or Master Administrators

FRU_FLT.1 Limited fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of ***all the TOE's capabilities, except possible loss of audit records,*** when the following failures occur: ***a High Availability cluster is configured and at least one HA passive screen is available before the active High Availability screen fails***.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: ***a High Availability cluster is configured and at least one HA passive screen is available before the active High Availability screen fails***.

5.1.2 TOE Security Assurance Requirements

The assurance security requirements for this Security Target taken from Part 3 of the CC, compose EAL2. These assurance components are summarized in the following table.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5.3 - Assurance Requirements: EAL2

ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user’s site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1 The developer shall test the TSF and document the results.

ATE_FUN.1.2 The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2 Rationale For Security Requirements

5.2.1 Rationale For Security Functional Requirements

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in this ST.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this ST depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA_ATD.1 User attribute definition

This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA_UAU.1 Timing of authentication

This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.1.1 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FMT_MSA.1 Management of security attributes (1)

This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to change specified security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

.

FMT_MSA.1 Management of security attributes (2)

This component ensures the TSF enforces the UNAUTHENTICATED_SFP to restrict the ability to create or delete specified security attributes that are listed in information flow rules in FDP_IFF.1(1). This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MSA.2 Secure security attributes

This component ensures that the TOE checks the security and validity of all security attributes. All IP addresses must be valid and in the correct format. All protocols must be defined by the system. All port numbers must be within the valid range of port numbers. All group memberships and identities must be defined. All passwords must be 6 to 8 characters in length. Values meeting these criteria are secure because they are defined to the extent need to implement access policies.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA and O.SECFUN.

FMT_MTD.1 Management of TSF data (1)

This component ensures that the TSF restricts abilities to query, modify, delete and assign certain user attributes as defined in FIA_ATD.1.1 to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN

FMT_MTD.1 Management of TSF data (2)

This component ensures that the TSF restricts abilities to set the time and date used to form timestamps to only the authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FCS_COP.1 Cryptographic operation (1), (2), (3), (4), (5)

These components ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that the identified cryptographic algorithms are used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FCS_CKM.1 Cryptographic key generation

This component ensures that the identified algorithm, Diffie-Hellman, generates the keys used to provide cryptographic operations. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FCS_CKM.4 Cryptographic key destruction

This component ensures that if cryptographic operations are used, destroyed keys are not accessible. The key destruction method used by SKIP is to overwrite old keys with new keys. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FMT_MOF.1 Management of security functions behavior

This component was to ensure the TSF restricts the ability to modify the behavior of functions such as startup and shutdown, audit trail management, back and restore for TSF data, and communication of authorized external IT entities with the TOE to an administrator with the appropriate, defined access level. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

FRU_FLT.1 Limited fault tolerance

This component ensures that TOE operation continues when a HA cluster is configured and at least one HA passive screen is available before the active High Availability screen fails. This component traces back to and aids in meeting all the IT security objectives. Single machines not part of a HA cluster do not have this ability.

FPT_FLS.1 Failure with preservation of secure state

This component ensures that the TOE preserves a secure state when a HA cluster is configured and at least one HA passive screen is available before the active High Availability screen fails. Single machines not part of a HA cluster do not have this ability. All High Availability systems must be on a HA dedicated network and must always be maintained identical to the active screen. The SunScreen EFS installation and configuration must be identical on each HA system.

This secure state definition should be considered secure because it requires that each passive screen be treated identical to the active screen in the event that the passive screen needs to become the active screen. This component traces back to and aids in meeting all the IT security objectives.

	O.IDAUTH	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_SMR.1								X	
FIA_ATD.1	X								
FIA_UID.2	X						X		
FIA_UAU.1	X								
FDP_IFC.1		X							
FDP_IFF.1		X							
FMT_MSA.1 (1)		X	X					X	
FMT_MSA.1 (2)		X	X					X	
FMT_MSA.2		X	X					X	
FMT_MSA.3		X	X					X	
FMT_MTD.1 (1)								X	
FMT_MTD.1 (2)								X	
FDP_RIP.1		X							
FCS_COP.1 (1)				X					
FCS_COP.1 (2)				X					
FCS_COP.1 (3)				X					
FCS_COP.1 (4)				X					
FCS_COP.1 (5)				X					
FCS_CKM.1				X					
FCS_CKM.4				X					
FPT_RVM.1					X				
FPT_SEP.1					X				
FPT_STM.1						X			
FAU_GEN.1						X	X		
FAU_SAR.1						X			
FAU_SAR.3						X			
FAU_STG.1					X			X	
FAU_STG.4					X			X	
FMT_MOF.1			X					X	X
FRU_FLT.1		X			X				
FPT_FLS.1		X			X				

Table 8.3 – Summary of Mappings Between Threats and IT Security Objectives

5.2.2 Rationale For Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.3 Rationale For Not Satisfying All Dependencies

The FCS_COP.1 functional components depend on the following functional components: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction and FMT_MSA.2 Secure Security Attributes. FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 have been included in this ST. FMT_MSA.2 depends on the following:

ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

The dependency for ADV_SPM.1 is not included due to the fact a clear definition of the secure values for the security attributes along with a reason why they should be considered secure is provided with the rationale for the FMT_MSA.2 security functional requirement in Section 5.2.1.

The FRU_FLT.1 functional component depends on the following functional component: FPT_FLS.1 Failure with preservation of secure state. FPT_FLS.1 depends on the following security assurance component: ADV_SPM.1 Informal TOE security policy model.

The dependency for ADV_SPM.1 is not included due to the fact a clear definition of the secure state along with a reason why it should be considered secure is provided with the rationale for the FPT_FLS.1 security functional requirement in Section 5.2.1.

5.4 IT Security Requirements on the Environment

In an evaluation, or other assessment of these non-TOE elements, the requirements listed are the minimal set that should be met to ensure correct operation of the TOE described in this security target. The following requirements should be met with an assurance component of EAL2 or greater.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behavior of all administrative functions*** to the ***authorized authentication server administrators.***

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role the ***authorized authentication server administrators.***

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.5 Rationale for IT Security Requirements on the Environment

The SecurID and Radius servers are relied upon to provide accurate information to the TOE to allow accurate I&A decisions to be made. While the servers are not part of the TOE, they must still be held accountable to the same assumptions and requirements regarding physical protection and self protection as other elements of the TOE, hence the inclusion of FPT_SEP.1 as a requirement on the environment. The other requirements are included as dependencies and sub-dependencies of FPT_SEP.1.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Access Control

The overall network access policy for the firewall is configured and enforced using a rule base. Access control policies within this TOE take the form of information flow control policies. The information flow control policy that is enforced for the SunScreen EFS Firewall is the packet filter policy (unauthenticated SFP). The packet filter policy includes the packet filtering rules, which provide no authentication at the firewall level. The unauthenticated SFP allows the passing of information from one user to another through the TOE. A protocol that has packet filtering rules setup may enforce its own access control, but this is not mandatory.

The packet filter policy provides the ability to filter network packets based on service (network service or service group), presumed source address, presumed destination address, transport layer protocol, network interface, certificate, and time. By default, SunScreen EFS drops any packet that does not have a specific Encryption or Allow action. If the packet filter allows the packet, network address translation can be performed.

The packet filter drops packets that are not conformant to the appropriate protocols or having IP level defects. This includes detecting and dropping malformed packets. Packets arriving on an interface with a presumed address that is not valid for that interface are dropped. This includes the following:

- packets arriving on the external TOE interface with a presumed source address on the internal network
- packets arriving on the internal TOE interface with a presumed source address on the external network
- packets arriving on the internal or external TOE interface with a presumed source address on the broadcast network
- packets arriving on the internal or external TOE interface with a presumed source address on the loopback network
- packets specifying routing information to the destination

The packet filter allows information flow and the passing or dropping of packets in support of the I&A process on behalf of the user being authenticated. An external or internal user may pass traffic through the TOE before authentication if the network access policy has a rule that allows the traffic to flow. Sending traffic through the TOE using the packet filtering mechanism is the only action a user may perform before authentication.

The firewall provides denial-of-service (DOS) protection by blocking traffic that is not allowed. The system is designed with kernel tables and denial-of-service (FIFO) storage methods that can grow when needed to prevent the firewall from becoming oversaturated with traffic.

Network address translation (NAT) enables a Screen to map an internal network address to a different network address. Static NAT maps a specific unregistered address to a specific registered address. Static translations can also map a range of unregistered addresses to a range of registered addresses, requiring the number of addresses in each range to match. Dynamic NAT maps a large set of unregistered IP addresses to a smaller set of registered addresses. Dynamic NAT creates a one-to-many mapping where several internal addresses use the same public address.

For packets traveling from the internal network through the Screen to the external network, the packet first passes through the packet filter. If the packet filter allows the packet and NAT is to be performed on the packet, the source IP address is converted. Next, based upon the action in the matched packet filter rule, the Screen determines whether or not the packet should be encrypted.

When the Screen receives a packet addressed to an internal host from a host on the external network, the Screen first passes encrypted packets to SKIP for decryption. Next, if NAT is to be performed on the packet, the destination IP address is converted. Finally, the packet passes through the packet filter to decide if the packet should be accepted or dropped.

6.1.2 Identification and Authentication

User authentication is based on a username and password pair, or a username and SecurID token, or both. The identification and authentication (I&A) security function is realized by a probabilistic mechanism For the I&A security function, the strength of function claim is SOF-basic. The SOF metrics defined for the I&A security function is:

> Strength of function shall be demonstrated for the mechanism used by the TOE to meet FIA_UAU.1 in that the probability that authentication data can be guessed is no greater than one in one million (1/E6).

Some special proxy user objects provide the means to map external collections of users into the SunScreen EFS access control facilities. SunScreen EFS provides administrative access to username/password and SecurID users.

SunScreen EFS can be configured to use SecurID authentication. SecurID's one-time password mechanism for hardware based authentication of administrators and users of the Screen. Because SecurID generates unpredictable, one-time- only access codes that automatically change during a set time period, reuse of a previously entered password is not feasible.

When configured to use SecurID for authentication, the TOE prevents reuse of authentication data related to authentication attempts from either an internal or external network by an authorized administrator, and authorized external IT entity or a human user attempting to access the services provided by the TOE.

SunScreen EFS provides two distinct levels of user identification: Authorized Users, through the `authuser` database, and Proxy Users, through the `proxyuser` database. The `authuser` database identifies individual administrative users of the firewall. The `proxyuser` database includes simple objects used to provide for and establish an association between an individual administrator and the role they play in usage of the facilities controlled by SunScreen, and group objects which are used to allow creation of groups of simple Proxy Users that share common access to facilities. Authorized Users and Proxy user names are distinct.

SunScreen EFS associates the following security attributes with individual users:

- identity
- group identity(ies)
- association with an administrative role
- authentication information (such as passwords, pins or tokens)

6.1.3 Secure Communication

The SunScreen firewall uses SunScreen Simple Key-Management for Internet Protocols (SKIP) to provide secure, encrypted communication between a remote Administration Station and the SunScreen firewall and between the SunScreen firewall and a remote SKIP host. The SunScreen firewall uses certificates when encrypting communications.

The firewall controls network access through the use of cryptographic identities. SunScreen EFS encrypts packets based on action values in the matching packet rules.

SKIP operates at the network IP layer and is transparent to virtually all applications. Secure communication is possible with all IP (TCP and UDP) applications without modification or knowledge of SKIP. SKIP uses the Diffie-Hellman key generation and distribution methods. Key destruction is performed by overwriting a newly generated key in the same memory location as the key being destroyed.

SunScreen EFS enables the creation of secure VPNs over public, insecure networks, such as the Internet. Encrypted tunnels protect the data transmitted between SKIP-enabled hosts or users, preventing unauthorized access to private data. The administrator selects what type of private-key and bulk-data encryption is to be used (such as RC2, RC4 or DES). For maximum security, SunScreen EFS uses SunScreen SKIP and Diffie-Hellman key pairs to encrypt the traffic key used for the bulk-data encryption and change the traffic key at frequent intervals. VPNs are implemented by the specific packet filter rules.

SKIP provides transparent encryption and authentication, which automatically encrypts and decrypts messages exchanged with other hosts running SKIP to ensure message privacy.

SKIP can provide cryptographic operations in accordance with the following algorithms and key sizes:

Encryption Algorithm	**Description**
DES-CBC	DES uses cipher block chaining (CBC) and a 56-bit key to encrypt 64-bit blocks of plaintext in multiple iterations.
DES-EDE-K3	DES-EDE-K3 (triple DES) uses three encryption operations and cipher block chaining (CBC) and a 56-bit key to encrypt 64-bit blocks of plaintext in multiple iterations.
RC2-40 (Restricted to 32-bit mode only for SKIP V1.5)	RC-2 uses cipher block chaining (CBC) and a variable-size key to encrypt 64-bit blocks of plaintext.
RC4-128	RC-4 uses a 128-bit key to encrypt data in a continuous stream.
RC4-40	RC-4 uses a 40-bit key to encrypt data in a continuous stream.

6.1.4 Security Audit

SunScreen EFS audits violations of the network access policy. SunScreen EFS provides flexible logging of packets. The firewall provides the ability to audit at the granularity of a single rule. Packets may be logged if they do or do not match a particular rule. The value of log size and information to be recorded in the administrative log files is established during the setup of the SunScreen EFS.

The SunScreen EFS log mechanisms provide the ability to inspect previously stored logs. By using the administrative GUI, a Screen’s active log file can be browsed in either historical or live modes. Logging allows authorized administrators to search, sort, and filter log messages to find critical information quickly and easily. The logs can be monitored using the browser and the command line in real time.

The administrator is provided with a powerful log filtering language. The filtering terms provide the ability to restrict the type of log events displayed based on network packet-type, network session-type, authentication events, policy editing, logging events, and event severity. Filtering is also provided based on the time, date, type of events, logging reason code, arrival interface name, destination hostname, origination hostname, service name, source or destination network, gateway used, and UDP, TCP, ICMP, and TCP protocol.

Log filters may also be defined as named quantities, refereed to as log macros. The advantages of log macros include uniform log filter availability, ease of common usage across a collection of managed Screens, and greater flexibility. Authorized administrators are able to scope the elements included in their log review through the use of macros.

Each audit record contains at least the following information:

a) Date and time of the event, type of event, subjects identities, outcome (success or failure) of the event; and

b) auditable event-specific information as described in Table 5.2.

If the audit trail is full, the oldest stored audit records are overwritten.

Operating system level logging is also provided by the Solaris Syslog. Syslog is used to log Solaris command line events, such as logging on and changing a user's Solaris password.

All log files are protected from unauthorized access (e.g., deletion and modification) because only administrators have direct access to the system.

The SunScreen firewall provides the following auditable events.

Component	**Description**	**Requirement Met**
FMT_SMR.1	Modifications to the group of users that are part of the **authorized administrator** role	Creation and modification of user identities and permissions are logged.
FIA_UID.2	All use of the user identification mechanism	Any use of the firewall authentication mechanisms is logged and the username is included.
FIA_UAU.1	Unsuccessful use of the authentication mechanism	Any use of the firewall authentication mechanisms is logged.
FDP_IFF.1	Decisions to permit requested information flows.	All decisions on requests for information flow are auditable. The source and destination of the presumed subject is captured in the audit record.
FCS_COP.1	Success and failure, and the type of cryptographic operation	Use of administrative functions is audited
FPT_STM.1	Changes to the time	Changes to the system time are auditable.
FMT_MOF.1a	Start-up and Shutdown	Startup and Shutdown of the TOE is logged

Component	Description	Requirement Met
FMT_MOF.1b	Create, delete, modify, and view security policies	All aspects of security policy creation and modification are auditable
FMT_MOF.1c	Create, delete, modify, and view user attributes	Changes to user attributes are auditable.
FMT_MOF.1d	Enable and disable single-use authentication mechanisms	All authentication attempts are auditable
FMT_MOF.1e	Authentication attempt failure	Attempts to authenticate to the TOE are auditable
FMT_MOF.1f	Restore authentication capabilities for disabled users	All actions related to users' accounts and privileges are auditable
FMT_MOF.1g	Enabling and disabling of external IT entity communication with TOE	Changes in TOE configuration are auditable
FMT_MOF.1h	Changes to time	Changes to the system time are auditable.
FMT_MOF.1i	Use of the audit trail	Access and use to the system logs is auditable
FMT_MOF.1k	Recovery to state	The ability to recover to state is a defined authorized administrator function.
FMT_MOF.1l	Remote administration	All actions related to remote administration are auditable.

6.1.5 Protection of the TSF

The following security functions describe the integrity and management functions that support the other security functions.

6.1.5.1 Time Stamps

The host OS provides reliable system time for use in filtering rules and audit.

6.1.5.2 Non-Bypassability

The TOE sits between an inside and an outside domain and implements a policy for distribution of network packets from one side to the other. All packets that enter the firewall are intercepted at the IP layer and screened against the related packet filtering and proxy rules. All other network methods for entering the TOE are disabled. The TOE only passes or discards packets based on the rules implemented, therefore network packets are never executed.

6.1.5.3 Domain Separation

SunScreen EFS provides two domains: an external domain and an internal domain. These domains are separated/enforced by the packet filter policy.

All processes executing on the TOE are trusted in that they are either the processes of administrative users, or are trusted processes implementing the policy. The TOE is not used for general purpose computing and does not allow untrusted users direct access. Untrusted users can interact with the TOE only through trusted entities such as the proxies. Domain separation is maintained because no untrusted subjects have access to the firewall.

6.1.5.4 Residual Data

Packets, buffers, and configuration rules created by the TOE will not contain residual data because they are completely overwritten with the new object when the packet, buffer, or rule is created.

6.1.6 Administration

SunScreen is administered either locally or remotely through either a command line interface or through a GUI interface. These SunScreen administrative accounts are different than normal SunScreen user accounts. Unless the administrator is the **root** user on the Screen, administrators must identify and authenticate themselves prior to performing administrative actions. Administering the Screen locally as the Solaris **root** user provides the user with SunScreen Master Administrative privilege.

The SunScreen EFS administrative interface supports four administrative access levels (roles):

Status	The ability to monitor systems, but not view the policies.
Local	The ability to read policies, but not change the policies. They must make a request for change to the Executive or Master administrators.
Executive	The ability to define and change policies.
Master	The ability to grant access levels to administrators.

Distinct administrator identities exist for the firewall administrative functions. An administrative utility is provided to allow the administrator to modify the firewall configuration and the network access policy.

The Solaris operating system is administered using the Solaris **root** account. If **ssadm** is executed locally by **root**, the user has Master administrative privilege. All administrative users, except Master administrators, must have normal Solaris user accounts (i.e., non-root accounts) since having a **root** account provides the user with Master administrative privilege.

The following administrative functions are provided by the SunScreen EFS administrative utilities.

a) start up and shutdown the TOE to the Master administrators;

b) enable or disable information flow security policy rules that permit or deny information flows, along with the security attributes in the rule, to the Executive or Master administrators;

c) enable or disable user attribute values defined in FIA_ATD.1 to the Master administrators;

d) enable or disable external IT entities communicating with the TOE to the Executive or Master administrators;

e) enable or disable single-use authentication to the Executive or Master administrators;

f) enable or disable remote administration from either an internal or external network to the Executive or Master administrators;

g) enable or disable addresses for remote administration to the Executive or Master administrators;

h) enable or disable individuals from being authorized remote administrators to the Master administrator;

i) view, modify, enable or disable access levels for remote administrators to the Master administrator.

j) view the audit trail to any of the administrators.

The security attributes set by the SunScreen EFS administrative interfaces are checked to ensure that they are secure and valid. SunScreen EFS provides restrictive default values for information security attributes used to enforce the policy.

Only Master administrators (**root**) shall be able to perform the following administrative functions:

- modify and set the system time and date
- manage the audit trails

SunScreen EFS provides centralized management of multiple Screens using a set of common objects through a specific, primary Screen. An administrator can also monitor logs on individual Screens or monitor logs of a centralized management group.

6.1.7 High Availability (HA)

HA contributes to protecting against denial of service attacks. It also enables the deployment of multiple screens in situations where the connection between a protected inside network and an insecure outside network is required. The active HA screen performs packet filtering, network address translation, logging, and encryption/decryption of packets traveling between the inside and outside networks. The other members of the HA cluster receive the same packets, perform the same calculations and mirror the state of the active HA screen, but they do not forward traffic. If the active HA screen fails, one of the passive screens takes over as the active and begins routing and filtering network traffic, preserving the secure state. This results in a few lost connections, loss of session state for proxy connections, and possible loss of audit records in the event of screen failure.

When setting up an HA cluster, one screen is designated as the primary HA screen and configured with the policy's configuration objects. When the security policy is activated, the policies are copied from the primary HA screen to the secondary screens. When a configuration is activated, the active screen transfers the configuration – including certificates, local keys, addresses, security policy rules, and more – to all other HA screens. Because the HA cluster transmits secret keys and policies in the clear over the dedicated HA network, HA networks must be kept physically secure.

6.2 Security Assurance Measures

The SUN EFS 3.0 firewall satisfies the assurance requirements for Evaluation Assurance Level 2 (EAL2). The following items will be provided as evidence:

Assurance Requirements	Assurance Measures
ACM_CAP.2	SunScreen™ EFS 3.0 Revision B Configuration Management and all its references.
ADO_DEL.1	SunScreen™ EFS 3.0 Revision B Delivery Document
ADO_IGS.1	SunScreen EFS 3.0 Revision B Installation Guide (Addendum to Sun Microsystems Installation Guide for SunScreen EFS 3.0) SunScreen™ EFS Release 3.0 Installation Guide – Revision B Binary Code License Start Here Release Notes

Assurance Requirements	Assurance Measures
ADV_FSP.1	SunScreen™ EFS 3.0 Functional Specification Routing Mode Operation, SunScreen™ EFS 3.0 High-Level Design Routing Mode Operation, Solaris ™2.6 man pages, Solaris™ 2.7 man pages, SKIP™ man pages.
ADV_HLD.1	SunScreen™ EFS 3.0 Functional Specification Routing Mode Operation, SunScreen™ EFS 3.0 High-Level Design Routing Mode Operation, SunScreen™ Technical White Paper.
ADV_RCR.1	SunScreen EFS 3.0 Revision B Representation Correspondence
AGD_ADM.1	SunScreen EFS 3.0 Revision B Installation Guide (Addendum to Sun Microsystems Installation Guide for SunScreen EFS 3.0) SunScreen EFS 3.0 Revision B Administrator Guide (Addendum to Sun Microsystems Administration Guide for SunScreen EFS 3.0) SunScreen™ EFS Release 3.0 Installation Guide – Revision B, Part #805-7744-11 SunScreen™ EFS Release 3.0 Administration Guide – Revision B part #805-7745-11 SunScreen™ SKIP User's Guide – Release 1.5 Revision B part #805-7875-11 Reference Manual part #805-7746-11
AGD_USR.1	SunScreen EFS Release 3.0 User's Guide – Revision B SunScreen™ SKIP User's Guide – Release 1.5 Revision B
ATE_COV.1	SunScreen EFS 3.0 Test Coverage Document
ATE_FUN.1	SunScreen EFS 3.0 Test Plans SKIP 1.5 Test Plans
ATE_IND.2	TOE Deliverable
AVA_SOF.1	SunScreen EFS 3.0 Strength of Function
AVA_VLA.1	SunScreen EFS 3.0 Vulnerability Analysis

Table – Summary of Mappings Between Assurance Measures and TOE Assurance Requirements

6.3 Rationale For Security Functions

The rationale for choosing SOF-basic is based on the low attack potential of threats identified by this ST. The security objectives provide probabilistic security mechanisms and the defined metric is satisfied by minimal industry standard password management features. Therefore these should satisfy SOF-basic.

FMT_SMR.1 Security roles

The Administration security function provides four administrative access levels and allows for the assignment of administrative access to identified users.

FIA_ATD.1 User attribute definition

The Administration security function manages user security attributes. The I&A security function maintains a database of user identities and security attributes.

FIA_UID.2 User identification before any action

The Administration security function requires users to authenticate to the administrative interface prior to performing any actions. The I&A security function performs the user identification requested by the Administration security function.

FIA_UAU.1 Timing of authentication

The I&A security function performs the user identification requested by the SunScreen EFS administrative interface. The access control security function allows authentication information to be passed to SunScreen EFS before users are authenticated. The packet filter and SunScreen EFS administrative interface ensure that users are authenticated at the TOE, however the packet filter does not perform authentication.

FDP_IFC.1 Subset information flow control (1)

The packet filter portion of the access control security function provides the ability to allow or deny the transmission of packets through the TOE.

FDP_IFF.1 Simple security attributes (1)

The packet filtering portion of the access control security function provides the ability to allow or deny the transmission of packets based on the subject and information security attributes.

FMT_MSA.1 Management of security attributes (1)

The Administration security function manages the rules of the unauthenticated SFP by restricting the ability to change security attributes for the packet filter.

FMT_MSA.1 Management of security attributes (2)

The Administration security function manages the rules of the unauthenticated SFP by restricting the ability to create or delete specified security attributes for the packet filter.

FMT_MSA.2 Secure security attributes

The Administration security function ensures the security and validity of all security attributes.

FMT_MSA.3 Static attribute initialization

By default, the packet filter portion of the access control security function implements a deny policy for the information flow control security rules. The Administration security function allows the Executive and Master administrators to configure information flow control security rules.

FMT_MTD.1 Management of TSF data (1)

The Administration security function restricts the ability to query, modify, delete and assign certain user attributes to the Master administrator.

FMT_MTD.1 Management of TSF data (2)

The Administration security function restricts the ability to set the system time and date to a Master administrator.

FDP_RIP.1 Subset residual information protection

The protection of TSF security function ensures that residual information is not included in data flowing within or external to the TOE.

FCS_COP.1 Cryptographic operation (1), (2), (3), (4), (5)

The Administration security function in cooperation with the packet filter portion of the access control security function ensures that remote administration traffic is encrypted. The Secure Communication security function performs the encryption and decryption of the network packets.

FCS_CKM.1 Cryptographic key generation

The Secure Communication security function generates new keys. The Administration security function provides administrators with an interface to install new keys and certificates.

FCS_CKM.4 Cryptographic key generation

The Secure Communication security function performs key destruction by overwriting old keys with the new keys.

FPT_RVM.1 Non-bypassability of the TSP

The protection of TSF security function ensures that the packet filter portion of the access control security function is located in the IP stack and cannot be bypassed.

FPT_SEP.1 TSF domain separation

The protection of TSF security function ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users.

FPT_STM.1 Reliable time stamps

The protection of TSF security function ensures that the date and time on the TOE is dependable.

FAU_GEN.1 Audit data generation

The audit security function records a minimal set of data with each audit records and provides a list of events that may be audited.

FAU_SAR.1 Audit review

The Administration security function provides an interface for reviewing the audit records in an understandable format.

FAU_SAR.3 Selectable audit review

The Administration security function provides an interface for searching and sorting the audit records.

FAU_STG.1 Protected audit trail storage

The audit security function ensures that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail.

FAU_STG.4 Prevention of audit data loss

The Administration and audit security functions ensure that the authorized administrator will be able to take care of the audit trail if it should become full. The audit security function also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status.

FMT_MOF.1 Management of security functions behavior

The Administration security function restricts the ability of the TOE management operations to an administrator with the appropriate, defined access level.

FRU_FLT.1 Limited fault tolerance

The High Availability security function ensures the operation of all the TOE's capabilities, except possible loss of audit records, when a HA cluster is configured and at least one HA passive screen is available before the active High Availability screen fails. Single machines not part of a HA cluster do not have this ability.

FPT_FLS.1 Failure with preservation of secure state

The High Availability security function ensures the preservation a secure state when a HA cluster is configured and at least one HA passive screen is available before the active High Availability screen fails. Single machines not part of a HA cluster do not have this ability.

	Access Control	I&A	Secure Communications	Security Audit	Protection of TSF	Administration	High Availability
FMT_SMR.1						X	
FIA_ATD.1		X				X	
FIA_UID.2	X	X				X	
FIA_UAU.1	X	X				X	
FDP_IFC.1 (1)	X						
FDP_IFC.1 (2)	X						
FDP_IFF.1 (1)	X						
FDP_IFF.1 (2)	X						
FMT_MSA.1 (1)						X	
FMT_MSA.1 (2)						X	
FMT_MSA.3	X					X	
FMT_MTD.1 (1)						X	
FMT_MTD.1 (2)						X	
FDP_RIP.1					X		
FCS_COP.1 (1)	X		X			X	
FCS_COP.1 (2)	X		X			X	
FCS_COP.1 (3)	X		X			X	
FCS_COP.1 (4)	X		X			X	
FCS_COP.1 (5)	X		X			X	
FCS_CKM.1	X		X			X	

	Access Control	I&A	Secure Communications	Security Audit	Protection of TSF	Administration	High Availability
FCS_CKM.4			X				
FPT_RVM.1					X		
FPT_SEP.1					X		
FPT_STM.1					X		
FAU_GEN.1				X			
FAU_SAR.1						X	
FAU_SAR.3						X	
FAU_STG.1				X			
FAU_STG.4				X		X	
FMT_MOF.1						X	
FRU_FLT.1						X	X
FPT_FLS.1						X	X

Table – Summary of Mappings Between IT Security Functions and TOE Security Requirements

6.4 Rationale For Security Assurance Measures

Each of the assurance measure documents was developed to satisfy the content and presentation of evidence elements of the mapped assurance requirement as defined in the CC.

Assurance Requirements	Assurance Measures	Assurance Rationale
ACM_CAP.2	SunScreen™ EFS 3.0 Revision B Configuration Management and all its references.	The configuration management documents contain all the information necessary to demonstrate that a CM system is used, that configuration items are defined, and that there is a unique reference for the TOE. The references contained within the document are the vendor's configuration management documentation provided to the product developers.
ADO_DEL.1	SunScreen™ EFS 3.0 Revision B Delivery Document	The delivery documents describes the process used to create distribution copies of the TOE, and the steps necessary to ensure consistent delivery of the TOE to the end user.

Assurance Requirements	Assurance Measures	Assurance Rationale
ADO_IGS.1	SunScreen EFS 3.0 Revision B Installation Guide (Addendum to Sun Microsystems Installation Guide for SunScreen EFS 3.0) SunScreen™ EFS Release 3.0 Installation Guide – Revision B Binary Code License Start Here Release Notes	The installation documentation describes the process necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	SunScreen™ EFS 3.0 Functional Specification for Routing Mode Operation SunScreen™ EFS 3.0 High-Level Design for Routing Mode Operation Solaris ™2.6 man pages Solaris™ 2.7 man pages SKIP™ man pages.	The functional specification documents completely represent the TSF and provides the purpose and method of use of all external TSF interfaces. The effects, exceptions, and error messages are documented.
ADV_HLD.1	SunScreen™ EFS 3.0 Functional Specification for Routing Mode Operation SunScreen™ EFS 3.0 High-Level Design for Routing Mode Operation SunScreen™ Technical White Paper.	The high-level design documents contain a representation of the TSF in terms of subsystems. The security functions are described. The subsystem interfaces are defined, and those that are externally visible are identified.
ADV_RCR.1	SunScreen EFS 3.0 Revision B Representation Correspondence	The representation correspondence maps the security functionality as described in the HLD, the FSP and the Security Target.

Assurance Requirements	Assurance Measures	Assurance Rationale
AGD_ADM.1	SunScreen EFS 3.0 Revision B Installation Guide (Addendum to Sun Microsystems Installation Guide for SunScreen EFS 3.0) SunScreen EFS 3.0 Revision B Administrator Guide (Addendum to Sun Microsystems Administration Guide for SunScreen EFS 3.0) SunScreen™ EFS Release 3.0 Installation Guide – Revision B, Part #805-7744-11 SunScreen™ EFS Release 3.0 Administration Guide – Revision B part #805-7745-11 SunScreen™ SKIP User's Guide – Release 1.5 Revision B part #805-7875-11 Reference Manual part #805-7746-11	The documents listed provide complete guidance to the TOE administrative personnel.
AGD_USR.1	SunScreen EFS Release 3.0 User's Guide – Revision B SunScreen™ SKIP User's Guide – Release 1.5 Revision B	The documents listed provide complete guidance to users of the TOE.
ATE_COV.1	SunScreen EFS 3.0 Test Coverage Document	The test coverage document provides a mapping of the testing performed against the TSF.
ATE_FUN.1	SunScreen EFS 3.0 Test Plans SKIP 1.5 Test Plans	The test plans and associated test cases provide the documentation of the vendor functional testing effort of the TOE.
ATE_IND.2	TOE Deliverable	The developer provided the TOE hardware and software.
AVA_SOF.1	SunScreen EFS 3.0 Strength of Function	The strength of function document provides the strength of function argument for Solaris passwords, SunScreen passwords, and SecurID.

Assurance Requirements	Assurance Measures	Assurance Rationale
AVA_VLA.1	SunScreen EFS 3.0 Vulnerability Analysis	The vulnerability analysis document provides the vendor's process for discovering obvious vulnerabilities. It also documents the vulnerabilities that resulted from executing the process.

Table –Assurance Measure Rationale

7 PP Claims

None.